

UNCLASSIFIED



# **NORTH DAKOTA HOMELAND SECURITY ANIT-TERRORISM SUMMARY**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

## **NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## **QUICK LINKS**

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including  
Schools and Universities\)](#)

[International](#)

[Information Technology and  
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials  
Sector](#)

[National Monuments and Icons](#)

[Commercial Facilities](#)

[Postal and Shipping](#)

[Communications Sector](#)

[Public Health](#)

[Critical Manufacturing](#)

[Transportation](#)

[Defense Industrial Base Sector](#)

[Water and Dams](#)

[Emergency Services](#)

[North Dakota Homeland Security  
Contacts](#)

UNCLASSIFIED

## **NORTH DAKOTA**

**Floodwaters shut down 30 oil wells in Williston area.** About 30 oil wells were shut off ahead of the rising water on the Missouri River west of Williston, North Dakota May 25, and a few of those wells are now under water. The head of the oil and gas division's Williston office, said he started alerting well operators May 23 to prepare for high water and found that several were on top of the situation. The Missouri River was expected to crest somewhere around 27.5 feet late May 25, slightly lower than anticipated. However, the high water put some wells under water, some partially under water, and some are now surrounded by water. He said well operators shut down the wells, removed any chemicals and motors from the site, and drained oil from tank batteries, refilling them with fluid so they would be too heavy to become buoyant. The spokesman said the wells were primarily older wells, but even at a 50-barrel per day, would cost the well owner a fair amount of money in lost production. The spokesman said damage to the electrical systems will be one of the major repair issues at the flooded wells. Source: [http://www.bismarcktribune.com/news/state-and-regional/article\\_ade9429a-8727-11e0-961d-001cc4c002e0.html](http://www.bismarcktribune.com/news/state-and-regional/article_ade9429a-8727-11e0-961d-001cc4c002e0.html)

**Problems continue along flooded Souris River in ND; campground evacuated, kayaker rescued.** High water continued May 23 to cause problems in the flooded Souris River basin in north central North Dakota. Water flooded some streets and basements in Minot, North Dakota May 23. A police spokeswoman told KCJB radio that water backed up from storm sewers that couldn't handle any more. The Minot Daily News reports that about 150 people were evacuated from a campground 2 miles west of Minot May 21. The owner of the Rough Rider Campground said a flooded access road thwarted efforts to bring in more clay to shore up dikes. He said he hoped the campground could reopen in about a week. Source: <http://www.dailyjournal.net/view/story/4ea04ffbdb5f49d5b102ae1571526132/ND--ND-Flooding-Souris-River/>

## **REGIONAL**

**(Minnesota) Health department issues warning on skin lightening products.** The Minnesota Department of Health is warning residents that some types of skin-lightening products may contain dangerous levels of mercury. Staff from St. Paul-Ramsey County Public Health tested 27 samples of products sold in the Twin Cities as skin-lightening agents and found 11 of the creams contained mercury at levels ranging from 135 to 33,000 parts per million. Under federal law, most cosmetics such as skin-lightening products can contain no more than trace amounts of mercury — less than 1 part per million. The state is asking consumers to not dispose of skin products that may contain mercury as normal trash. A statewide list of disposal sites for hazardous materials is available on the Minnesota Pollution Control Agency's Web site. At a minimum, consumers should make sure the products they are using have ingredient lists, and that mercury is not listed. Mercury may appear on labels under different names, the state said, so consumers should check for the words "calomel," "mercuric," "mercurous" or "mercurio."

## UNCLASSIFIED

The primary health concern with exposure to mercury in skin creams is the potential effect on the kidneys, according to the health department, but exposure to high levels of mercury or exposure over long periods of time can raise other concerns. Source:

[http://www.twincities.com/ci\\_18137431?nclick\\_check=1](http://www.twincities.com/ci_18137431?nclick_check=1)

**(Minnesota) Federal jury convicts Burnsville man of bilking mortgage lenders out of more than \$43 Million.** A jury convicted a 44-year-old Burnsville, Minnesota man in federal court May 24 on seven counts of wire fraud, three counts of mail fraud, and one count of conspiracy to commit wire fraud and mail fraud in a scheme that bilked mortgage lenders out of more than \$43 million. The evidence presented at trial indicated that between 2005 and 2008, the man conspired with others to obtain money fraudulently through over 100 residential property transactions. To further this scheme, the conspirators negotiated with builders of new properties as well as owners of existing properties to buy property and property groupings at greatly reduced prices. They then solicited real estate purchasers by promising they would receive large cash pay-outs, or "kickbacks," from lenders' funds. They failed to tell potential buyers about the reduced prices they negotiated for the properties, choosing instead to quote them the grossly inflated prices. By charging buyers the higher prices, they acquired enough cash from loan proceeds to pay buyers their kickbacks and still have money left for themselves and their co-conspirators. Once a potential buyer was recruited through this scheme, the conspirators, or someone working on their behalf, drafted a purchase agreement that reflected the inflated sale price only and failed to disclose to lenders the kickback amount to the buyer. The convict faces a potential maximum penalty of 20 years in federal prison on each count. Source: <http://minneapolis.fbi.gov/dojpressrel/pressrel11/mp052411a.htm>

**(Montana) Police jackets stolen from unmarked car.** Eleven Billings, Montana Police Department investigations division jackets and a radio were stolen from an unmarked police car on the West End either May 21 or 22. The police sergeant said the car was parked at an officer's house and had two boxes of jackets and the radio inside. The new jackets were supposed to be given to officers May 23. The suspect made off with one of the jackets and an EF Johnson radio. The jackets are black with "Billings Police Investigations Division" embroidered on the front left side and "Police/Investigations Division" written on the back in yellow. The police sergeant said anyone who feels suspicious about someone wearing a similar jacket can ask to see a badge or identification. Source: [http://billingsgazette.com/news/local/crime-and-courts/blogs/crime-watch/article\\_b578213d-f811-54f7-9f7c-4777698e66f3.html](http://billingsgazette.com/news/local/crime-and-courts/blogs/crime-watch/article_b578213d-f811-54f7-9f7c-4777698e66f3.html)

## **NATIONAL**

**Ohio couple pleads guilty to conspiring to finance Hezbollah.** A married couple from Toledo, Ohio, pleaded guilty May 23 to charges related to a plan to send hundreds of thousands of dollars to Hezbollah. The couple met multiple times between August 2009 and June 2010 with a confidential source working on behalf of the Federal Bureau of Investigation, during which time they discussed ways to secretly send money to Hezbollah leaders in Lebanon, court documents said. The confidential source delivered \$200,000 to the couple June 3, 2010, and told them he

UNCLASSIFIED

## UNCLASSIFIED

would return later in the day with more money, court documents said. Shortly thereafter, the couple was seen inside their home bundling a portion of the money in plastic wrap and duct tape to prepare it for concealment. The wife pleaded to one count of conspiracy, and the husband to a total of five counts that included conspiracy to provide support to a foreign terrorist organization, and conspiracy to violate money laundering law. Source: <http://blogs.wsj.com/corruption-currents/2011/05/23/ohio-couple-pleads-guilty-to-conspiring-to-finance-hezbollah/>

## **INTERNATIONAL**

**Pirates plead guilty in killings.** Three Somalis have pleaded guilty in the piracy that led to the killings of four U.S. citizens aboard the yacht Quest in February. All of the three suspects entered guilty pleas in federal court in Norfolk, Virginia May 20. The charges carry mandatory life sentences. In their plea agreements, the three men said they "played no role in the murder of the four United States citizens." Source: [http://www.upi.com/Top\\_News/US/2011/05/21/Pirates-plead-guilty-in-killings/UPI-10711305982905/](http://www.upi.com/Top_News/US/2011/05/21/Pirates-plead-guilty-in-killings/UPI-10711305982905/)

**Hundreds of flights canceled as ash cloud hits.** Airlines clashed with regulators and pilots May 24 as passengers braced themselves for days of uncertainty and chaos caused by a volcanic ash cloud being blown across the British Isles. England's weather service said ash from Iceland's Grimsvotn volcano had moved over parts of Scotland, prompting air regulators to warn airlines they had to seek permission to fly to and from the area. Hundreds of flights were canceled in Britain and Ireland. A weather service spokesman said volcanic ash had been detected on the ground in Scotland, and a special laser based on the Shetland Islands northeast of the Scottish mainland also detected ash in the atmosphere. "All the data we are receiving confirms our forecasts, that there is high-density ash over Scotland," he said. Experts said particles in the ash could stall jet engines and sandblast planes' windows. Irish budget airline Ryanair immediately challenged the results. It said it sent its own airplane into Scottish airspace and found no ash. The main international body representing carriers, the International Air Transport Association, complained to the British government about the way it had handled the issue, saying it should have had Cessna planes ready to carry out tests, instead of relying on the weather service. But other airlines were more willing to follow official advice. The spokesman for Aer Lingus, said it had canceled 20 flights between Ireland and Scotland. Source: <http://www.msnbc.msn.com/id/43148143/ns/travel/?GT1=43001>

**Manitoba dike resealed but rain a worry.** The cut in a protective dike at the Hoop and Holler Bend on the Assiniboine River in Manitoba, Canada, is sealed, but with rain in the forecast, officials said the release of water could yet happen again, Canadian Broadcasting Corporation reported May 21. The dike was breached May 14 as part of a plan to ease pressure on other flood-protection systems on the swollen river. The breach created a flood of its own, but not as severe as might have occurred with an uncontrolled break somewhere else on the river. The Assiniboine River is at record high levels from spring run-off. In the latest flood bulletin, issued

UNCLASSIFIED

## UNCLASSIFIED

by the province May 21, officials said the breach was sealed around noon May 20. "There is a remote possibility that the release point could be reopened if there are issues on the Portage Diversion channel or along the Assiniboine River dikes," the province reported. Residents in the controlled release area were being told to maintain their flood protection structures for at least another week. Source: <http://www.cbc.ca/news/canada/manitoba/story/2011/05/21/mb-flood-update-110521.html>

**Envoys rescued from embassy in Yemen.** An armed mob loyal to Yemen's embattled president surrounded an embassy May 22, trapping the American and other ambassadors inside for hours until they apparently were flown out in a Yemeni military helicopter. The president May 22 balked at signing the agreement drawn up by the Gulf Cooperation Council (GCC), as armed mobs took to the streets of the capital, Sanaa, and surrounded an embassy where at least five U.S., European, and Arab envoys were meeting about the crisis, according to witnesses and news reports. The president's supporters massed outside the United Arab Emirates Embassy, blocking two entrances and at one point attacking a convoy bringing the GCC's top mediator to the compound, news agencies reported. Mobs surrounded other foreign embassies; the Chinese ambassador's convoy also came under attack, according to news reports. Source: [http://seattletimes.nwsourc.com/html/nationworld/2015123366\\_yemen23.html](http://seattletimes.nwsourc.com/html/nationworld/2015123366_yemen23.html)

**Small blast rattles Northern Ireland's Londonderry.** Masked men, allegedly shouting they were members of the Irish Republican Army, abandoned a small bomb and fled a commercial area in Londonderry, Northern Ireland, the mayor said May 21. The mayor said the bomb was carried into the office of the Santander bank on Shipquay Street May 21 by the men who immediately fled the scene. The bomb, which exploded an hour later, did not cause injuries or substantial damage, he said. Northern Ireland, historically plagued by sectarian violence between Catholics and Unionist Protestants, has seen a resurgence of violence recently. Source: [http://articles.cnn.com/2011-05-21/world/n.ireland.bomb\\_1\\_ira-splinter-group-irish-republican-army-ireland-republicans?s=PM:WORLD](http://articles.cnn.com/2011-05-21/world/n.ireland.bomb_1_ira-splinter-group-irish-republican-army-ireland-republicans?s=PM:WORLD)

**Total 250 tons of radioactive water leaked into sea early May: TEPCO.** Highly contaminated radioactive water that leaked into the sea earlier in May from a pit near a seawater intake of the No. 3 reactor at Japan's Fukushima Daiichi nuclear power plant totaled 250 tons and contained an estimated 20 terabecquerels of radioactive substances, Tokyo Electric Power Co (TEPCO) said May 21. The estimated amount of radioactive substances from the plant, crippled by the March 11 earthquake and ensuing tsunami, is about 100 times the annual allowable limit for release outside the plant, the company said. The leak is estimated to have lasted for 41 hours from 2 a.m. May 10 through 7 p.m. the following day, TEPCO said based on its analysis of data showing changes in water levels in the pit. The leak from near the No. 3 reactor compares with about 500 tons of radioactive water with 4,700 terabecquerels of radioactive substances that leaked from near the No. 2 reactor from April 1 to 6. Source: <http://www.japantoday.com/category/national/view/total-250-tons-of-radioactive-water-leaked-into-sea-early-may-tepco>

## UNCLASSIFIED

## **BANKING AND FINANCE INDUSTRY**

Nothing Significant to Report

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**Regulators find design flaws in new reactors.** In a setback for the only model of nuclear reactor for which ground has been broken in the United States, government regulators have found additional problems with the design of its shield building, a crucial component, the chairman of the Nuclear Regulatory Commission said May 20. He said computations submitted by Westinghouse, the manufacturer of the new AP1000 reactor, about the building's design appeared to be wrong and "had led to more questions." He said the company had not used a range of possible temperatures for calculating potential seismic stresses on the shield building in the event of an earthquake, for example. Earlier in 2011, the commission staff said it needed additional calculations from Westinghouse to confirm the strength of the AP1000's shield building. The Southern Company has already dug the foundations and done other preliminary work for two of the AP1000 reactors adjacent to its existing reactors at Plant Vogtle near Augusta, Georgia. South Carolina Electric and Gas has broken ground for another two, 20 miles northwest of Columbia. In addition to the plants in Georgia and South Carolina, ground has also been broken on four AP1000 reactors in China, two at Sanmen, and two at Haiyang. Source:

[http://www.nytimes.com/2011/05/21/business/energy-environment/21nuke.html?\\_r=2&bl=&pagewanted=all](http://www.nytimes.com/2011/05/21/business/energy-environment/21nuke.html?_r=2&bl=&pagewanted=all)

**U.S. needs more training for nuclear inspectors: NRC.** U.S. citizens may be at risk from radioactive waste stored near nuclear plants as better training for federal safety inspectors and more on-site checks are needed, an internal government report showed May 20. The Nuclear Regulatory Commission's (NRC) inspector general said in an audit the NRC needs a formal, agency-wide training program to ensure its inspectors can do the best job when checking spent fuel storage sites. The inspector general looked at the NRC's oversight of spent fuel storage installations, which generally consist of a concrete pad that holds used fuel inside steel cylinders surrounded by additional steel or concrete. The audit said the NRC does not require classroom training in concrete technology, the use of cranes for heavy loads, and welding inspection techniques. The report said some NRC inspectors believe it is acceptable to walk around the perimeter of a dry cask storage pad. Other inspectors insist on walking onto the pad to assess the condition of the casks and make sure the cooling vents on the containers are not blocked, it said. The inspector general also said the NRC must define how far apart inspections should be. Inspections varied from 1 to almost 6 years, with many occurring every 2 years.

Source: <http://www.reuters.com/article/2011/05/20/us-usa-nuclear-inspectors-idUSTRE74J6UH20110520>

## **COMMERCIAL FACILITIES**

(California) **ATF determines Stockton mosque fire was arson.** Federal investigators have determined a fire that destroyed a mosque in Stockton, California, in April was arson. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) announced its findings May 25. The ATF had opened an investigation into the fire at the Masjid Al-Emaan Mosque after it was gutted April 23. The mosque was located in a strip mall. A church next door, Living Well Ministries and Christian Center, was also damaged in the blaze. Damage from the fire was estimated to be about \$400,000. There were no injuries. No arrests have been made, but authorities are hoping a \$10,000 reward for information will lead them to a suspect, or suspects. Source: <http://www.sacbee.com/2011/05/25/3654810/atf-determines-stockton-mosque.html>

**Powerful storms pound several central US states.** In storm-weary middle America, many people counted themselves lucky May 26 after powerful storms swept through the region for the third time in 4 days but apparently claimed no lives. Dozens of people were injured, mobile homes were flipped, and roofs were torn off houses when tornadoes and thunderstorms hit Indiana, Illinois, Missouri, and other states May 25. Authorities began assessing the storm damage after daybreak, tallying up the number of homes damaged and destroyed. More than a dozen people were injured, including several children. A tornado damaged many homes and businesses May 25 in the Missouri city of Sedalia, causing minor injuries to as many as 25 people. Heavy rain, hail, and lightning pounded Memphis, Tennessee, May 25 as a tornado warning sounded. There were no confirmed reports of tornadoes. Elsewhere in Tennessee, strong winds from thunderstorms damaged homes and wrecked a convenience store in Smithville, about 55 miles east of Nashville. In Illinois, strong winds, rain, and at least four possible tornadoes knocked down power lines, and damaged at least one home and a number of farm buildings across the central and eastern parts of the state. Source: <http://www.chron.com/disp/story.mpl/ap/top/all/7582412.html>

(Connecticut; New York) **Bridgeport man accused of selling pipe bombs in NYC.** A 37-year-old Connecticut man was charged May 20 with five counts of making, transporting and selling explosives and firearms after selling eight sticks stuffed with ball bearings and explosive material from his car in a Bronx, New York parking lot to an undercover police officer for \$3,200 May 19. Bomb-making material was also found inside the man's apartment in Bridgeport, Connecticut, an FBI spokesman said. A bomb squad technician was injured when a small jar containing a white powdery residue exploded while he was examining it. The technician suffered minor injuries and was released from an area hospital, the FBI said. Authorities said agents also identified about 15 flashlights that a bomb technician at the scene said appeared to have been adapted to form a destructive device. They also saw three photographs of between 50 and 80 cylindrical objects with fuses that appeared similar in size to those the man sold. The FBI said there was no evidence of ties to terrorism in the case. Source: <http://www.courant.com/community/bridgeport/hc-bridgeport-bomb-making-0521-2-20110520,0,6582030.story>

## UNCLASSIFIED

**Man held in car bomb probe deported to Pakistan.** A Pakistani man arrested in Massachusetts during the investigation of the failed New York Times Square car bombing in Manhattan, New York, was deported to Pakistan May 22, federal authorities said. The 28-year-old was accompanied by Immigration and Customs Enforcement officers on a flight from Logan International Airport in Boston to Islamabad, Pakistan, the agency said in a statement. The man pleaded guilty in April to immigration and illegal money-transfer charges and was sentenced to time served. He did not face terrorism-related charges. Prosecutors alleged the suspect gave \$4,900 to the man who was later convicted in the bombing attempt. Source: <http://www1.whdh.com/news/articles/local/12004379413620/man-held-in-car-bomb-probe-deported-to-pakistan/>

### **COMMUNICATIONS SECTOR**

**(Connecticut) Texas men charged after trooper finds them on tower.** Two men from Texas who got around a barbed-wire fence and climbed the communications tower at Mohawk State Forest in Cornwall, Connecticut were arrested May 23. State police said a 20-year-old man, of Spring Branch, and the 26-year-old man, of Fredericksburg, were in the tower when a state trooper spotted lights flickering from it while he was on routine patrol. The 20-year-old was charged with second-degree criminal trespass and delivery of alcohol to a minor. The 26-year-old was charged with possession of drug paraphernalia, possession of a controlled substance, possession of liquor and second-degree criminal trespass. They were both held overnight on \$5,000 bond and arraigned May 23 in Bantam Superior Court. Police said there was no apparent damage to the communications tower. Source: <http://www.rep-am.com/news/local/doc4ddba0f75b4cf660150141.txt>

### **CRITICAL MANUFACTURING**

**Walmart recalls GE food processors due to laceration and fire hazard.** Walmart Stores Inc., of Bentonville, Arkansas, issued a recall May 25 for about 255,000 General Electric food processors. The safety interlock system on the recalled food processor can fail; allowing operation without the lid secured which poses a laceration hazard. Also, the product can emit smoke, or catch fire, posing a fire hazard. Walmart has received a total of 58 incident reports: 24 reports of the food processor operating without the lid in place, of which 21 resulted in injuries to fingertips; and 34 reports of the unit smoking, including 3 reports of fires. The recall involves GE-branded digital, 14-cup food processors. The food processors are black with stainless steel trim, and model number 169203 is imprinted on the underside of the unit. The food processors were sold exclusively at Walmart stores nationwide, and Walmart.com from September 2009 through February 2011. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml11/11227.html>

UNCLASSIFIED

## UNCLASSIFIED

**STIHL recalls yard power products due to burn and fire hazards.** STIHL Inc., of Virginia Beach, Virginia, issued a recall May 25 for 2.3 million trimmers, brushcutters, KombiMotors, hedge trimmers, edgers, clearing saws, pole pruners, and backpack blowers that utilize a toolless fuel cap. The level of ethanol and other fuel additives can distort the toolless fuel cap, allowing fuel to spill, posing a fire and burn hazard. STIHL has received 81 reports of difficulty installing and/or removing the fuel caps and fuel spillage. No injuries have been reported. The yard power products were sold at authorized STIHL dealers nationwide from July 2002 through May 2011. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml11/11226.html>

## **DEFENSE/ INDUSTRY BASE SECTOR**

**Pentagon agency halts kill vehicle production.** The U.S. Missile Defense Agency (MDA) suspended production of the latest version of the Exoatmospheric Kill Vehicle (EKV), part of the Ground Based Midcourse Defense (GMD) anti-ballistic-missile system, while it looks into a 2010 flight test failure, the agency's director said. In May 25 testimony before the Senate Appropriations Committee's defense panel, the director also said a plan to shift program oversight of the U.S. Army's Patriot air and missile defense system to MDA could be in place as soon as 2013. The GMD interceptor missile, which failed during the final moments of a test last December, was an upgraded version of the currently deployed GMD system. This upgraded version includes a new EKV, the Raytheon-built component that intercepts an incoming missile in space. The suspension will last until required design modifications are completed and verified, and the agency has diverted 2011 GMD funding to expedite the modifications. Source: <http://www.defensenews.com/story.php?i=6621589&c=AME&s=AIR>

**The Pentagon confronts new enemy: rust.** The U.S. Navy's Mega Rust 2011 conference is set to be held in June, Wired reported May 23. This annual get-together of military personnel, government officials, researchers, manufacturers, and suppliers seeks to share knowledge and advance understanding of how to deal with the corrosion of military hardware. Currently, rust costs the Defense Department \$23 billion a year, and affects everything from old jets, tankers, and bombers to Naval ships and planes. Even dealing with rust on the Air Force's F-22 is expected to cost millions. Combined with better maintenance, new technologies could cut costs by 30 percent over 20 years, an official with the Defense Department's Corrosion Office said. Named CorrDefense, the office was established in 2003 to eliminate rust from military hardware. Source: <http://www.wired.com/dangerroom/2011/05/the-pentagon-declares-war-on-rust/>

## **EMERGENCY SERVICES**

**(California) Supreme Court orders California prisoner release.** The U.S. Supreme Court May 23 ordered California to release tens of thousands of inmates or take other steps to ease overcrowding in its prisons to prevent "needless suffering and death." By a 5-4 vote, the high

## UNCLASSIFIED

## UNCLASSIFIED

court told the nation's largest state prison system to sharply cut its inmate population in stages over 2 years in one of the biggest prison release orders in U.S. history. A Justice said for the court majority that the medical and mental health care provided by California's prisons had fallen below the standard of decency required by the U.S. Constitution. He cited suicidal inmates being held for prolonged periods in telephone booth-sized cages, backlogs of up to 700 prisoners waiting to see a doctor for care, and as many as 54 inmates sharing a single toilet. California's 33 adult prisons were designed to hold about 80,000 inmates and now have about 145,000. Because of prison population reductions while the case has been on appeal, the Justice calculated the state may have to release 37,000 more inmates or take other measures, such as putting low-risk offenders into community-based programs, and building more prisons.

Source:

<http://www.myvictoriaonline.com/pages/9900428.php?contentType=4&contentId=8210377>

## **ENERGY**

**Researcher blasts Siemens for downplaying SCADA threat.** The security researcher who voluntarily canceled a talk on critical vulnerabilities in Siemens' industrial control systems the week of May 16 took the German company to task May 23 for downplaying the problem. The researcher, with NSS Labs, took exception to Siemens' claim the vulnerabilities he and a colleague uncovered had been discovered "while working under special laboratory conditions with unlimited access to protocols and controllers." "There were no 'special laboratory conditions' with 'unlimited access to the protocols.' My personal apartment on the wrong side of town where I can hear gunshots at night hardly defines a special laboratory," he said in a message posted on a public security mailing list. "[And] I purchased the controllers with money my company so graciously provided me with." While Siemens promised the week of May 16 that it would patch the bugs, it downplayed the threat to its industrial control systems, and the thousands of companies that rely on Siemens' programmable logic control systems, the researcher argued. Source:

[http://www.computerworld.com/s/article/9216994/Researcher\\_blasts\\_Siemens\\_for\\_downplaying\\_SCADA\\_threat](http://www.computerworld.com/s/article/9216994/Researcher_blasts_Siemens_for_downplaying_SCADA_threat)

## **FOOD AND AGRICULTURE**

**(Georgia) E. coli recall: 500 pounds of ground beef.** A Georgia retailer is recalling about 500 pounds of ground beef products that may be contaminated with E. coli, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced May 25. The problem at Food Depot #24, of McDonough, Georgia, was discovered through routine FSIS monitoring, which confirmed a positive result for E. coli O157:H7, the FSIS said. The recalled beef, produced May 19, was sold at Food Depot #24 store in McDonough. The beef was sold in 1-lb.- to 4-lb.-tray packs with a "sell by" date of May 20, 2011. Source:

<http://www.foodsafetynews.com/2011/05/e-coli-recall-500-pounds-of-ground-beef/>

## UNCLASSIFIED

## UNCLASSIFIED

**FDA: Do not feed SimplyThick to premature infants.** The U.S. Food and Drug Administration (FDA) is advising parents, caregivers, and health care providers not to feed SimplyThick, a thickening product, to premature infants. The product may cause necrotizing enterocolitis (NEC), a life-threatening condition. FDA first learned of adverse events possibly linked to the product May 13. To date, the agency is aware of 15 cases of NEC, including 2 deaths, involving premature infants who were fed SimplyThick for varying amounts of time. The product was mixed with mothers' breast milk or infant formula products. Illnesses have been reported from at least four different medical centers. The illnesses involve premature infants who became sick over the past 6 months. SimplyThick was added to the feeding regimen of infants — who later developed NEC — to help with swallowing difficulties stemming from complications of premature birth. Parents and caregivers who have medical concerns or concerns or questions related to the use of the product should contact their health care provider. The product is sold in packets of individual servings and in 64-ounce dispenser bottles. It can be purchased from distributors and local pharmacies throughout the United States. Source:

<http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm256253.htm>

**Listeria test prompts cheese recall.** Atalanta Corp. of Elizabeth, New Jersey, recalled some bulk cheese because it may be contaminated with *Listeria monocytogenes*. In a news release, the company said that after routine testing by the Belgium manufacturer revealed the presence of *Listeria monocytogenes*, the company recalled less than 70 cases of its "Nazareth Classic" and "Nazareth Light" cheeses. The cheeses were distributed mostly in North East retail stores. Recall notices were sent to retail outlets that received the potentially affected product. All remaining inventory was quarantined and will be destroyed under U.S. Food and Drug Administration supervision. No illnesses were reported. Source:

<http://www.foodsafetynews.com/2011/05/listeria-test-prompts-cheese-recall/>

**(Illinois) Salad suspected in Illinois salmonella outbreak.** Although health department investigators have not been able to pinpoint the cause of a salmonella outbreak in St. Charles, Illinois, they said evidence suggests it was the salad at Portillo's restaurant. Fifteen people have been confirmed infected with the outbreak strain of salmonella, according to a news release May 23 from the Kane County Health Department. Eleven of the case patients reported eating at Portillo's, and 7 of those reported eating a salad. It is not known how the salad might have become contaminated. Food samples collected from the restaurant all tested negative. Two Portillo's employees tested positive for *Salmonella* Typhimurium, but investigators identified them as likely victims of the outbreak, not the source. So far, 76 employees have been cleared to return to work after twice testing negative in tests conducted 48 hours apart. The onset of the first illness was April 5, and onset of the last illness was April 30. Three of the case patients became so ill they were hospitalized. Kane County said it will work with the Illinois Department of Public Health and the DuPage, DeKalb, and Chicago health departments in investigating the outbreak. Source: <http://www.foodsafetynews.com/2011/05/salad-suspected-in-illinois-salmonella-outbreak/>

## UNCLASSIFIED

## UNCLASSIFIED

**Honeybees continue to die off at 'unsustainable' level.** Winter losses of honeybees impacted by still-unexplained die-offs remained about the same as the previous 5 years, but the level still concerns beekeepers in Pennsylvania. About 30 percent of managed honeybee colonies across the nation died between October and April, according to a preliminary analysis of an annual survey conducted by the U.S. Department of Agriculture (USDA) and the Apiary Inspectors of America. Winter losses have ranged from 29 percent to 36 percent since late 2006. "That's unsustainable," a senior extension associate and bee expert at Penn State University said. "The lack of increase in losses is marginally encouraging in the sense that the problem does not appear to be getting worse for honeybees and beekeepers," a USDA entomologist who helped conduct the study said in a news release. "But continued losses of this size put tremendous pressure on the economic sustainability of commercial beekeeping." Beekeepers reported that losses of 13 percent would be economically acceptable, the survey said. Average colony losses for individual beekeepers was about 38 percent, down from 42 percent in 2010. Survey reports were fielded from 5,572 beekeepers who manage more than 15 percent of the country's estimated 2.7 million colonies. Source:

[http://www.pittsburghlive.com/x/pittsburghtrib/news/s\\_738560.html](http://www.pittsburghlive.com/x/pittsburghtrib/news/s_738560.html)

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**(Colorado) Suspicious letter shuts down revenue department building.** A suspicious piece of mail emptied the Colorado Department of Revenue's office building May 25. About 500 people employed there were evacuated after a letter containing a suspicious white powder was discovered at the building across the street from the Colorado State Capitol. A hazardous materials team joined Denver firefighters and police in the investigation, which determined the substance to be benign. "There was an envelope with powder in it, but it turned out not to be dangerous," said a spokesman for the governor's office. Police closed Sherman Street between 13th and 14th avenues for about 90 minutes beginning at 9:45 a.m., when the powder was discovered. Department of revenue employees re-entered the building around 11 a.m. Source:

[http://www.chieftain.com/suspicious-letter-shuts-down-revenue-department-building/article\\_560e9700-86fa-11e0-a840-001cc4c002e0.html](http://www.chieftain.com/suspicious-letter-shuts-down-revenue-department-building/article_560e9700-86fa-11e0-a840-001cc4c002e0.html)

**(New York) Another suspicious package sent to Sen. Ball.** The Putnam County Sheriff's Office in New York continued its investigation May 23 into a suspicious package that was delivered in the evening May 20 to the Route 22 office of a state senator, forcing authorities to shut down the road in Southeast for about 3 hours while the Westchester County Bomb Squad investigated. Authorities finally determined the package was not a threat and that it contained a book on the values of the Prophet Muhammad and other Islamic views. It also contained a letter to the senator voicing concerns over a recent legislative hearing he chaired in New York City. In April, a Georgia woman mailed a suspicious package to the senator's Albany office. It contained a stuffed Curious George monkey pinned with Stars of David and a vicious, anti-Semitic, and racially charged letter. Source:

## UNCLASSIFIED

## UNCLASSIFIED

<http://www.lohud.com/article/20110525/NEWS01/105250329/Another-suspicious-package-sent-Sen-Ball?odyssey=mod|newswell|text|News|s>

**IRS staff committed tax credit fraud.** According to federal investigators, more than 100 employees of the Internal Revenue Service (IRS) cheated the government by fraudulently claiming a first-time homebuyer tax credit included in the 2008 and 2009 economic stimulus packages, the Washington Times reported May 23. The Treasury Department's inspector general for tax administration, in several reports over the past few years, identified a total of 128 IRS employees who claimed the credit but who also made other claims that showed they either were not first-time buyers or bought their homes outside the eligibility period for the credit, which was worth up to \$8,000. The IRS employees represented a small part of the total fraud in the program, which the inspector general said may have totaled more than \$500 million overall. At least one IRS employee is facing charges of making a false claim while acting as an officer of the government — a felony punishable by up to 5 years in prison — stemming from the tax credit. In another case, a part-time IRS employee in Georgia has been charged with altering information on IRS computers to help four friends and family members appear eligible for the credit. She pleaded guilty March 24 to one count of accessing a computer without authorization and is awaiting sentencing. Source:

<http://www.washingtontimes.com/news/2011/may/23/irs-staff-committed-tax-credit-fraud/?page=all#pagebreak>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**Rogue VirusTotal Website distributes Java malware.** Security researchers from antivirus vendor Kaspersky Lab have come across a fake VirusTotal Web site that is being used to distribute malware via a Java-based downloader. VirusTotal is a popular service that allows users to scan files with many antivirus engines. The site is used by hundreds of thousands of professionals and regular users on a daily basis. The spoofed site discovered by Kaspersky looks exactly like the real one and prompts users to run a Java applet. Because the applet is not signed with a valid certificate, users are asked to confirm its execution. The applet is actually a Java-based trojan downloader that distributes a piece of malware detected by Kaspersky as Worm(dot)MSIL.Arcdoor.ov. The botnet is controlled through a commercial Web-based DDoS framework known as NOise. It accepts commands to initiate several types of DDoS, report the hostname of the victim machine, type, and version of the operation system, as well as the version of the malware itself. Source: <http://news.softpedia.com/news/Rogue-VirusTotal-Website-Distributes-Java-Malware-202387.shtml>

**Timing attack threatens private keys on SSL servers.** Security researchers have discovered a "timing attack" that creates a possible mechanism for a hacker to extract the secret key of a TLS/SSL server that uses elliptic curve cryptography (ECC). Elliptic curve cryptography is a type of public-key algorithm that uses the maths of elliptic curves rather than integer factorization, which is used by RSA as a one-way function. By using ECC, it is possible to provide equivalent levels of difficulty for a brute-force attack as can be provided by the more familiar integer-factorization approaches, but using smaller key lengths. The approach has benefits for mobile

## UNCLASSIFIED

## UNCLASSIFIED

and low-power systems. Two researchers discovered some implementations of ECC are vulnerable to a form of side-channel attack based on measuring the length of time it takes to digitally sign a message. The attack can be carried out locally or, with greater difficulty, remotely. The researchers validated their research through tests on an OpenSSL Server running ECC they had established, as explained in the abstract of a research paper by the computer scientists. Source:

[http://www.theregister.co.uk/2011/05/25/elliptic\\_curve\\_crypto\\_security\\_attack/](http://www.theregister.co.uk/2011/05/25/elliptic_curve_crypto_security_attack/)

**Exploited Hotmail bug stole email without warning.** Microsoft has patched a bug in its Hotmail e-mail service that attackers were exploiting to silently steal confidential correspondences and user contacts from unsuspecting victims. The vulnerability was actively being exploited using e-mails that contained malicious scripts, a Trend Micro researcher said May 23. Successful attacks required only that a Hotmail user open the malicious e-mail or view it in a preview window. The commands embedded in the e-mails uploaded users' correspondences and user contacts to servers under the control of attackers without requiring the victim to click on links or otherwise take any action. The scripts also had the capability of enabling e-mail forwarding on the targeted Hotmail account, allowing attackers to view e-mails sent to the victim in the future.

Source: [http://www.theregister.co.uk/2011/05/24/microsoft\\_hotmail\\_email\\_theft\\_attack/](http://www.theregister.co.uk/2011/05/24/microsoft_hotmail_email_theft_attack/)

**Mac App Store's slow updates expose users to security risks.** Apple's Mac App Store puts users at risk because it is slow to update vulnerable software, a security researcher said May 18. The researcher noted the Opera browser had not been updated on the Mac App Store since March 1. Since May 18, however, Opera has released two updates to add features, fix crash bugs, and patch vulnerabilities. Opera updated to version 11.11 May 18, which closed a critical hole that could be exploited by attackers to infect a Mac with malicious code. "Users who rely on the App Store to tell them whether their software is up-to-date may not be aware of the security risks and may continue to use an unsafe version of the Opera browser," the researcher said. When Apple launched the Mac App Store in January 2010, one of the online mart's selling points was it would automatically notify customers when updates were available. The researcher's argument is Apple failed to make good on the promise. "Mac users who have downloaded Opera through the App Store may find themselves using a copy of Opera that is now two versions old," he said. Source:

[http://www.computerworld.com/s/article/9216860/Mac\\_App\\_Store\\_s\\_slow\\_updates\\_expose\\_users\\_to\\_security\\_risks](http://www.computerworld.com/s/article/9216860/Mac_App_Store_s_slow_updates_expose_users_to_security_risks)

**New 64-bit rootkit being used to steal banking credentials.** Security researchers have come across a new rootkit designed specifically to infect 64-bit Windows systems and steal users' online banking credentials. It is believed to be the first piece of malware of its kind that is capable of compromising x64 systems. The new rootkit is being used by attackers in Brazil as part of drive-by download attacks and is then used to steal banking credentials after the infection. The malware has the ability to change some of the boot configurations of infected machines and then aims to redirect users to phishing sites. The new rootkit can infect machines running either 32-bit or 64-bit versions of Windows. The drive-by download is accomplished by using a malicious Java applet targeted at older versions of the Java Runtime Environment. The

## UNCLASSIFIED

## UNCLASSIFIED

applet includes a number of files that each have different jobs to do once they are on an infected PC, including one that disables the Windows User Account Control mechanism. Source: [http://threatpost.com/en\\_us/blogs/new-64-bit-rootkit-being-used-steal-banking-credentials-052011](http://threatpost.com/en_us/blogs/new-64-bit-rootkit-being-used-steal-banking-credentials-052011)

**Sony security breaches keep on popping up.** A new Sony security breach has been reported, involving user information being leaked from the Web site of Sony BMG Greece. The incident was revealed the weekend of May 21 and 22 when someone publicly disclosed the stolen information of 8,385 users. However, the actual compromise occurred earlier in May. The database dump was publicly posted on pastebin.com and it contained usernames, e-mail addresses, passwords, and in some cases telephone numbers. "It appears someone used an automated SQL injection tool to find this flaw. It's not something that requires a particularly skillful attacker, but simply the diligence to comb through Sony Web site after Web site until a security flaw is found," a security advisor at Sophos said. SQL injection vulnerabilities are very common, and Sony is not the only large company caught with such holes in its Web properties. Two other Sony compromises revealed the week of May 16 include the stealing of gift points worth \$1,225 from 128 So-net Entertainment accounts, and the discovery of a phishing page hosted on Sony's Thailand portal. Source: <http://news.softpedia.com/news/Sony-Security-Breaches-Keep-on-Popping-Up-201675.shtml>

**Another DoS fix for Apache HTTP server.** The update of the Apache HTTP Server (httpd) to version 2.2.18 earlier in May to close a denial of service (DoS) problem appears to have exposed a related DoS vulnerability. The developers released httpd 2.2.19 to fix this new problem that has been rated as moderately critical; however, as with the previous DoS vulnerability, it requires that mod\_autoindex is enabled in the Web server. It appears the updated Apache Portable Runtime (APR) 1.4.4 — undled with the server to correct the denial of service vulnerability — could cause httpd workers to enter a 100 percent CPU utilizing hung state when calling apr\_fnmatch. An update to APR, version 1.4.5, which resolves the issue has been released by the APR developers and is bundled with Apache HTTP Server 2.2.19. Users can upgrade to httpd 2.2.19 or, if running httpd 2.2.17 or earlier, work around the denial of service problem by using the "IgnoreClient" option of the "IndexOptions". The problem was first noted and tracked on Debian mailing lists. Source: <http://www.h-online.com/security/news/item/Another-DoS-fix-for-Apache-HTTP-server-1247712.html>

## **NATIONAL MONUMENTS AND ICONS**

**(Arizona; New Mexico) Wildfire along southern AZ/NM border grows to 40,000 acres, still 25 percent contained.** A human-caused wildfire along the Arizona-New Mexico border has grown to more than 40,000 acres. The U.S. Forest Service said the Horseshoe Two wildfire was 25 percent contained as of May 23. Burnout operations continued May 22 in an attempt to rob the wildfire of dead grass and trees. Fire crews were in place at a research station, and the community of Paradise west of Portal in southeast Arizona. A precautionary evacuation order for the community of Paradise was in place as crews conducted nearby burnout operations.

## UNCLASSIFIED

## UNCLASSIFIED

Source: <http://www.therepublic.com/view/story/1443fdb5a7054558998493b44a6af043/AZ--Arizona-Wildfire/>

### **POSTAL AND SHIPPING**

Nothing Significant to Report

### **PUBLIC HEALTH**

**Smallpox-destruction deadline gets delayed.** Global health officials May 24 delayed setting a deadline for the destruction of the last known stocks of smallpox for at least 3 more years, a compromise that will enable scientists in the United States and Russia to continue researching medicines to counter a potential bioterror attack using smallpox. The consensus at the World Health Assembly, the decision-making body of the World Health Organization, came after a contentious debate over 2 days. The United States, Russia, and more than two dozen other countries in the developed and developing world had supported a resolution to keep the stocks of the deadly virus for at least an additional 5 years. It also required countries aside from the United States and Russia to declare to the WHO they did not hold stocks of live smallpox virus. Iran, China, Thailand, and other countries objected to the resolution, and wanted an earlier timetable. The question now is at what point global officials will agree they no longer need the virus to develop medicines to protect the public against a potential bioterror attack using smallpox, or an accidental release of the virus. Source:

<http://online.wsj.com/article/SB10001424052702304520804576343072510493118.html>

**CDC warns against exposure to 'mad cow'-like brain diseases.** U.S. researchers have new data about how humans are exposed to "prion" diseases, which are rare, progressive conditions that affect brain function, such as variant Creutzfeldt-Jakob disease, chronic wasting disease, and bovine spongiform encephalopathy, commonly known as "mad cow disease." The study, published in the June issue of the Journal of the American Dietetic Association, found that eating wild deer meat (venison) is one of the most common ways people are exposed to these serious, debilitating diseases. In examining the results of a 2006-2007 population survey conducted by the Foodborne Diseases Active Surveillance Network (FoodNet), U.S. Centers for Disease Control researchers were able to track how participants may have been exposed to prion diseases. Investigators found that 29.5 percent of those polled traveled to at least one of the nine countries where bovine spongiform encephalopathy was widespread, with England being the most common destination (19.4 percent of survey participants). Travelers to England were also more likely to stay longer. In fact, nearly one-quarter remained in the country for at least a month. Moreover, 18.5 percent of those polled hunted for deer, and 1.2 percent hunted for elk in regions known for chronic wasting disease. Venison was eaten by 67.4 percent of those surveyed. Of those who ate deer meat, 88.6 percent got it from the wild. Source:

<http://www.wsfa.com/Global/story.asp?S=14699182>

## UNCLASSIFIED

## **TRANSPORTATION**

**(New York) NYPD investigates shooting on MTA bus in Brooklyn.** The New York City Police Department (NYPD) was asking for the public's help as they investigate a shooting on a Metropolitan Transit Authority (MTA) bus in Brooklyn. Police responding to a 911 call May 18 found an 18-year-old African-American man shot once in the torso on a B60 bus at Stanhope Street and Central Avenue in Bushwick. They arrived on the scene around 4:40 p.m. Emergency services personnel brought the victim to Elmhurst Hospital, where he was listed in stable condition. The suspect was caught on surveillance tape. Police described him as an 18-year-old African-American man wearing a light blue Holister sweatshirt. Source: <http://newyork.cbslocal.com/2011/05/19/nypd-investigates-shooting-on-mta-bus-in-brooklyn/>

**(Louisiana) Coast Guard may partially reopen portion of Mississippi River to barge traffic Monday.** The U.S. Coast Guard may partially reopen a 9-mile segment of the Mississippi River to barge traffic as it reviews a plan to remove three barges that sank in the waterway in Baton Rouge, Louisiana, the week of May 16. A petty officer said the Coast Guard expects to allow northbound traffic on the river to resume sometime May 23. Southbound barges would be allowed to travel down the river once the northbound backup is cleared. Archer Daniels Midland Co., which owns the barges involved in the May 20 accident, has submitted a plan for salvaging the wreckage. They were part of a 20-barge tow that was being pushed downriver amid high water and fast currents that have made navigation difficult. One of the barges struck a dock while two others struck a bridge. Source: <http://www.greenfieldreporter.com/view/story/be213aeed87047fa81426e7c982002c7/LA--River-Flooding-Louisiana/>

## **WATER AND DAMS**

**Three Gorges Dam blamed for China's worst drought in 50 years.** China's Three Gorges Dam began disgorging about 5 billion cubic meters of water May 26 to replenish the Yangtze River and counter Hubei's lowest rainfall in half a century. Without it, rice and grain production would be in jeopardy. Now power output is expected to drop just as consumption hits its summertime high. Seven central and eastern provinces, plus Shanghai, are experiencing water shortages. Authorities blame the problem on global warming, but many experts point the finger at the 185-meter-high Three Gorges Dam. Since it came on stream, droughts are more frequent and longer lasting. China has a vast network of hydroelectric dams, and the driest season in 50 years is causing unexpected difficulties. Water levels at the Danjiangkou Dam on the Han River, a tributary of the Yangtze, have dropped to a record low. In almost 1,600 reservoirs in Hubei province, there is 40 percent less water than a year ago, already one of the driest years on record. Nearly 10 million people in 87 cities and counties have been hit by the prolonged drought, and 1.2 million hectares of farmland are suffering from chronic water shortages. Lake

## UNCLASSIFIED

Poyang (Jianxi), China's largest, has shrunk to less than a fifth of its usual area. Source: <http://www.asianews.it/news-en/Three-Gorges-Dam-blamed-for-China%27s-worst-drought-in-50-years-21663.html>

**(Louisiana) Mandatory evacuation order lifted.** In Louisiana, the mandatory evacuation order for residents living south of U.S. 190, the Three Mile Lake area and the North Wilderness Road area has been lifted, the St. Landry Parish president announced May 23. The areas will remain under voluntary evacuation until further notice, and a mandatory evacuation order remains in effect all for all livestock and residents on the east side of the levee. The president asked the 335 residents affected by the evacuation zones not to bring furniture and evacuated items back into their homes yet because another mandatory evacuation may be issued. The St. Landry Parish Sheriff's Department will continue patrolling the voluntary evacuation areas and preparing for possible flooding. Along with the sheriff's deputies, the National Guard, U.S. Coast Guard and U.S. Army Corps of Engineers will keep a presence in areas at risk of flooding. According to a deputy district commander with the New Orleans District Corps of Engineers, 17 floodgates of the Morganza Spillway were open as of May 23. The floodgates reroute water from the swollen Mississippi River into the Atchafalaya Basin to prevent further strain on Baton Rouge and New Orleans levee systems. The Corps will continue observing Mississippi River levels to determine if more gates will be opened. Source: <http://www.dailyworld.com/article/20110524/NEWS01/105240317/Mandatory-evacuation-order-lifted>

## **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov); Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security [kihagel@nd.gov](mailto:kihagel@nd.gov), 701-328-8168

UNCLASSIFIED